Listing of the Claims

The following listing of claims will replace all prior versions and listings of the claims in the application:

1. (Currently Amended) A ~~crypto~~ cryptographic algorithm unit comprising:

a first ~~crypto~~ cryptographic hash execution module; and

a second ~~crypto~~ cryptographic hash execution module, wherein the first ~~crypto~~ cryptographic execution module and the second ~~crypto~~ cryptographic execution module share a plurality of components to form a combination ~~crypto~~ cryptographic algorithm unit, wherein the combination ~~crypto~~ cryptographic algorithm unit being capable of performing an MD5 hash algorithm and a SHA1 hash algorithm, the combination ~~crypto~~ cryptographic algorithm unit including:

a first summing circuit, the first summing circuit being a four input summing circuit with a single first summing circuit output, wherein the first summing circuit includes a four to two compressor and a first carry look-ahead adder wherein the four to two compressor is a two output device and the two outputs are coupled to each of two inputs to the first carry look-ahead adder, the first carry look-ahead adder having the first summing circuit output, wherein the four to two compressor has a vector length independent propagation delay of less than four XOR gates;

a second summing circuit, the second summing circuit being a second two input carry look ahead adder:

wherein a first input to the second summing circuit is coupled to the first summing circuit output, wherein the first summing circuit output is coupled to the first input to the second summing circuit through a rotate circuit during an MD5 hash algorithm;

wherein a SHA1 chaining variable is coupled to the second input to the second summing circuit during a SHA1 hash algorithm; and

wherein an MD5 chaining variable is coupled to the second input to the second summing circuit during an MD5 hash algorithm.

2. (Currently Amended) The ~~crypto~~ cryptographic algorithm unit of claim 1,

wherein the combination ~~crypto~~ cryptographic algorithm unit includes a plurality of ~~muxes~~ multiplexers.

3. (Currently Amended) The ~~crypto~~ cryptographic algorithm unit of claim 2, wherein the plurality of ~~muxes~~ multiplexers provides a ~~crypto~~ cryptographic hash algorithm selection control.

4. (Currently Amended) The ~~crypto~~ cryptographic algorithm unit of claim 3, wherein the ~~crypto~~ cryptographic hash algorithm selection control allows the selection of a first subset of the plurality of components, wherein the selected first subset of the plurality of components can execute a first ~~crypto~~ cryptographic algorithm.

5. (Canceled)
6. (Canceled)

7. (Currently Amended) The ~~crypto~~ cryptographic algorithm unit of claim 1, wherein the second ~~crypto~~ cryptographic hash execution module is capable of executing at least one of a group of ~~crypto~~ cryptographic hash algorithms consisting of the SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm that is different from the ~~crypto~~ cryptographic hash algorithm that the first ~~crypto~~ cryptographic hash execution module is capable of executing.

8. (Currently Amended) The ~~crypto~~ cryptographic algorithm unit of claim 1, wherein the combination ~~crypto~~ cryptographic algorithm unit is on a single integrated circuit die.

9. (Currently Amended) The ~~crypto~~ cryptographic algorithm unit of claim 1, wherein the combination ~~crypto~~ cryptographic algorithm unit and a microprocessor are on a single integrated circuit die.

10. (Currently Amended) The ~~crypto~~ cryptographic algorithm unit of claim 1, wherein the combination ~~crypto~~ cryptographic algorithm unit includes one or more full adders.

11. (Canceled)

12. (Currently Amended) The ~~crypto~~ cryptographic algorithm unit of claim 1, wherein the combination ~~crypto~~ cryptographic algorithm unit includes a plurality of compressors.

13. (Canceled)

14. (Currently Amended) An integrated circuit comprising:

a microprocessor core; and

a combination ~~crypto~~ cryptographic algorithm unit, the combination ~~crypto~~ cryptographic algorithm unit being coupled to the microprocessor core wherein the combination ~~crypto~~ cryptographic algorithm unit includes a first ~~crypto~~ cryptographic execution module and a second ~~crypto~~ cryptographic hash execution module, wherein the first ~~crypto~~ cryptographic execution module and the second ~~crypto~~ cryptographic execution module share a plurality of components, wherein the combination ~~crypto~~ cryptographic algorithm unit being capable of performing an MD5 hash algorithm and at least one of a group of cryptographic hash algorithms consisting of a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm ~~a SHA1 hash algorithm~~, the combination ~~crypto~~ cryptographic algorithm unit including:

a first summing circuit, the first summing circuit being a four input summing circuit with a single first summing circuit output, wherein the first summing circuit includes a four to two compressor and a first carry look-ahead adder wherein the four to two compressor is a two output device and the two outputs are coupled to each of two inputs to the first carry look-ahead adder, the first carry look-ahead adder having the first summing circuit output, wherein the four to two compressor has a vector length independent propagation delay of less than four XOR gates;

a second summing circuit, the second summing circuit being a second two input carry look ahead adder:

wherein a first input to the second summing circuit is coupled to the first summing circuit output, wherein the first summing circuit output is coupled to the first input to the second summing circuit through a rotate circuit during an MD5 hash algorithm;

wherein a SHA1 chaining variable is coupled to the second input to the second summing circuit during a SHA1 hash algorithm; and

wherein an MD5 chaining variable is coupled to the second input to the second summing circuit during an MD5 hash algorithm.

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Currently Amended) The integrated circuit of claim 14, wherein the second ~~crypto~~ cryptographic hash execution module is capable of executing at least one of a group of ~~crypto~~ cryptographic hash algorithms consisting of the SHA-1 hash algorithm, a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm that is different from the ~~crypto~~ cryptographic hash algorithm that the first ~~crypto~~ cryptographic hash execution module is capable of executing.

19. (Currently Amended) A method of executing a ~~crypto~~ cryptographic instruction comprising:

receiving a first ~~crypto~~ cryptographic hash instruction in a combination ~~crypto~~ cryptographic algorithm unit;

determining a corresponding first ~~crypto~~ cryptographic hash algorithm for the first ~~crypto~~ cryptographic instruction;

selecting a first plurality of components in the combination ~~crypto~~ cryptographic algorithm unit including a first ~~crypto~~ cryptographic execution module and a second ~~crypto~~ cryptographic hash execution module, wherein the first ~~crypto~~ cryptographic execution module and the second ~~crypto~~ cryptographic execution module share a plurality of components, wherein the combination ~~crypto~~ cryptographic algorithm unit being capable of performing an MD5 hash algorithm and at least one of a group of cryptographic hash algorithms consisting of a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm ~~a SHA1 hash algorithm~~, the combination ~~crypto~~ cryptographic algorithm unit including:

a first summing circuit, the first summing circuit being a four input summing circuit with a single first summing circuit output, wherein the first summing circuit includes a four to two compressor and a first carry look-ahead adder wherein the four to two compressor is a two output device and the two outputs are coupled to each of two inputs to the first carry look-ahead adder, the first carry look-ahead adder having the first summing circuit output, wherein the four to two compressor has a vector length independent propagation delay of less than four XOR gates;

a second summing circuit, the second summing circuit being a second two input carry look ahead adder:

wherein a first input to the second summing circuit is coupled to the first summing circuit output, wherein the first summing circuit output is coupled to the first input to the second summing circuit through a rotate circuit during an MD5 hash algorithm;

wherein a SHA1 chaining variable is coupled to the second input to the second summing circuit during a SHA1 hash algorithm; and

wherein an MD5 chaining variable is coupled to the second input to the second summing circuit during an MD5 hash algorithm; and

executing the first ~~crypto~~ cryptographic hash instruction through the selected first plurality of components.

20. (Currently Amended) The method of claim 19, further comprising:

receiving a second ~~crypto~~ cryptographic hash instruction in the combination ~~crypto~~ cryptographic algorithm unit;

determining a corresponding second ~~crypto~~ cryptographic hash algorithm for the second ~~crypto~~ cryptographic hash instruction;

selecting a second plurality of components in the combination ~~crypto~~ cryptographic algorithm unit; and

executing the second ~~crypto~~ cryptographic hash instruction through the selected second plurality of components, the selected second plurality of components and the selected first plurality of components sharing a third plurality of components.

21. (New) The cryptographic algorithm unit of claim 7, wherein the first cryptographic hash execution module is capable of executing at least one of a group of cryptographic hash algorithms consisting of a SHA256 hash algorithm, a SHA384 hash algorithm, and a SHA512 hash algorithm.